

Sidon Sequences and Doubly Periodic Two-Dimensional Synchronization Patterns

Tuvi Etzion

Department of Computer Science
Technion-Israel Institute of Technology
Haifa 32000, Israel
Email: etzion@cs.technion.ac.il

Abstract—Sidon sequences and their generalizations have found during the years and especially recently various applications in coding theory. One of the most important applications of these sequences is in the connection of synchronization patterns. A few constructions of two-dimensional synchronization patterns are based on these sequences. In this paper we present sufficient conditions that a two-dimensional synchronization pattern can be transformed into a Sidon sequence. We also present a new construction for Sidon sequences over an alphabet of size $q(q-1)$, where q is a power of a prime.

I. INTRODUCTION

Let \mathcal{A} be an abelian group and let $\mathcal{D} = \{a_1, a_2, \dots, a_m\} \subseteq \mathcal{A}$ be a subset of m distinct elements of \mathcal{A} . \mathcal{D} is a *Sidon sequence* (or a B_2 -sequence) over \mathcal{A} if all the sums $a_{i_1} + a_{i_2}$ with $1 \leq i_1 \leq i_2 \leq m$ are distinct (if $i_1 < i_2$ in the definition the sequence is called a *weak Sidon sequences*). Sidon sequences have found many applications in coding and communication. For example, weak Sidon sequences are used for construction of constant weight codes with minimum Hamming distance 6 [1], and constructions of location-correcting codes [2]. Sidon sequences were used in constructions of two-dimensional synchronization patterns [3], [4]. There is a generalization to B_h sequences (all sums of h elements are distinct) and they applied for example in multihop paths related to wireless sensor networks [5] and error-correcting codes for rank modulation [6]. A comprehensive survey on B_2 -sequences and their generalizations was given by O'Bryant [7]. Even so in a Sidon sequence all sums of pairs of elements from \mathcal{D} (not necessarily distinct elements) are distinct there is a trivial connection to a set in which all differences of ordered pairs of elements are distinct.

Theorem 1: A subset $\mathcal{D} = \{a_1, a_2, \dots, a_m\} \subseteq \mathcal{A}$ is a Sidon sequence over \mathcal{A} if and only if all the differences $a_{i_1} - a_{i_2}$ with $1 \leq i_1 \neq i_2 \leq m$ are distinct in \mathcal{A} .

A Sidon sequence with m elements over an abelian group with n elements is called *optimal* if all Sidon sequences over an abelian group with n elements have at most m elements. In view of Theorem 1 bounds on the size of a Sidon sequence (on the number of elements m) can be derived by considering difference and not sums. This is important since the number of distinct sums is $\binom{m}{2} + m = \frac{m^2+m}{2}$ while the number of distinct differences is considerably higher, $m(m-1) = m^2 - m$. This yields a better upper bound on m . A Sidon sequence \mathcal{D} is a set of m elements. If the abelian

group is \mathbb{Z}_n then \mathcal{D} can be represented as a binary cyclic sequence $s = [s_0 s_1, \dots, s_{n-1}]$, where $s_i = 1$ if $i \in \mathcal{D}$.

One-dimensional synchronization patterns were first introduced by Babcock in connection with radio interference [8]. Other applications are discussed in details in [9] and some more are given in [10], [11]. The two-dimensional applications and related structures were first introduced in [12] and discussed in many papers, e.g. [13], [14], [15], [16], [17]. Recent new application in keys predistribution for wireless sensor networks [18] led to new related two-dimensional problems concerning these patterns [3], [5]. Difference pattern and Sidon sequences have an important role in the construction of synchronization patterns.

Some of the applications of Sidon sequence is due to the difference properties implied by Theorem 1. This property is also the basis of the applications to two-dimensional synchronization patterns. There are various papers, e.g. [3], [4], [17] in which an one-dimensional sequence (as a Sidon sequence or a ruler) is transformed into a two-dimensional synchronization pattern. The main goal of this paper is to establish the inverse transformation, in which a two-dimensional synchronization pattern is transformed into a Sidon sequence, which is a one-dimensional sequence.

The rest of this paper is organized as follows. In Section II we define what is a period in a two-dimensional array and as a result we obtain a definition for a cyclic two-dimensional array. In Section III we discuss various types of two-dimensional synchronization patterns. In particular we discuss periodic two-dimensional synchronization patterns. In Section IV we present two operations, namely, folding and unfolding. Folding generates a two-dimensional array from an one-dimensional sequence. Unfolding is the inverse operation and it generates an one-dimensional sequence from a two-dimensional array. In particular we will prove that these operations relate periodic sequences to periodic two-dimensional arrays and vice-versa. Moreover, they relate an one-dimensional synchronization sequence to a two-dimensional synchronization array and vice-versa, if the two-dimensional array is periodic. As a consequence we obtain the main result of the paper that two-dimensional periodic synchronization arrays which can be unfolded are equivalent to Sidon sequences over \mathbb{Z}_n , where n is the size of one period in the array. In Section V we present a construction of optimal Sidon sequences with $q-1$ elements over a group with $q(q-1)$ elements, where q is a power of a prime. This

generalizes a similar result where q is a prime. Section VI contains conclusions and problems for further research.

II. PERIODICITY OF TWO-DIMENSIONAL ARRAYS

A. periodic sequences and arrays

It is very simple to define the periodicity for one-dimensional sequences. An infinite sequence $S = \dots s_{-1}, s_0, s_1, s_2, \dots$ is periodic if there exists an integer π such that $s_{i+\pi} = s_i$ for each $i \in \mathbb{Z}$. If π is the smallest integer for which the sequence has this property then we say that π is the *period* of the sequence and write the sequence as $[s_0, s_1, \dots, s_{\pi-1}]$, and say that the sequence is a *cyclic sequence* or a *cycle*. It is well known that

Theorem 2: If π is the period of a sequence S , and there exists an integer ρ such that $s_{i+\rho} = s_i$ for each $i \in \mathbb{Z}$, then π divides ρ .

Usually, an infinite two-dimensional array \mathcal{A} is said to be doubly periodic if there exists two integers κ and η such that for each $i, j \in \mathbb{Z}$ we have $\mathcal{A}(i + \kappa, j) = \mathcal{A}(i, j + \eta) = \mathcal{A}(i, j)$. But, it appears that this definition is too restricted. A generalized definition, which give more information, is as follows. An infinite two-dimensional array A is *doubly periodic* if there exists two linearly independent integer vectors (π_1, π_2) and (ξ_1, ξ_2) such that each $i, j \in \mathbb{Z}$ satisfy $\mathcal{A}(i + \pi_1, j + \pi_2) = \mathcal{A}(i + \xi_1, j + \xi_2) = \mathcal{A}(i, j)$. How we can define the smallest vectors with this property? What is the period of the array? and what is a cyclic two-dimensional array? These questions will be answered after two necessary definitions, of tiling and lattices, will be presented.

B. Tiling

Tiling is one of the most basic concepts in combinatorics. We say that a two-dimensional shape S tiles the two-dimensional square grid \mathbb{Z}^2 if disjoint copies of S cover \mathbb{Z}^2 . This cover of \mathbb{Z}^2 with disjoint copies of S is called a *tiling* of \mathbb{Z}^2 with S . For each shape S , in the tiling, we distinguish one of the points of S to be the *center* of S . Each copy of S in a tiling has the center in the same related point. The set \mathcal{T} of centers in a tiling defines the tiling, and hence the tiling is denoted by the pair (\mathcal{T}, S) . Given a tiling (\mathcal{T}, S) and a grid point (i_1, i_2) we denote by $c(i_1, i_2)$ the center of the copy of S , S' , for which $(i_1, i_2) \in S'$. We will also assume that the origin is a center of a copy of S . The first lemma given in [4] can be easily verified.

Lemma 1: For a given tiling (\mathcal{T}, S) and a point (i_1, i_2) the point $(i_1, i_2) - c(i_1, i_2)$ belongs to the shape S whose center is in the origin.

C. Lattices and Lattice Tiling

One of the most common types of tiling is a *lattice tiling*. A two-dimensional *lattice* Λ is a discrete, additive subgroup of the real two-dimensional space \mathbb{R}^2 . W.l.o.g., we can assume that

$$\Lambda = \{u_1 v_1 + u_2 v_2 : u_1, u_2 \in \mathbb{Z}\} \quad (1)$$

where v_1, v_2 are two linearly independent vectors in \mathbb{R}^2 . A lattice Λ defined by (1) is a sublattice of \mathbb{Z}^2 if and only if

$\{v_1, v_2\} \subset \mathbb{Z}^2$. We will be interested solely in sublattices of \mathbb{Z}^2 . The vectors v_1, v_2 are called *basis* for $\Lambda \subseteq \mathbb{Z}^2$, and the 2×2 matrix

$$\mathbf{G} = \begin{bmatrix} v_{11} & v_{12} \\ v_{21} & v_{22} \end{bmatrix}$$

having these vectors as its rows is said to be the *generator matrix* for Λ . Note, that it is always possible to use a generator matrix \mathbf{G} in which all the four entries are nonzeros. It is also always possible to have in \mathbf{G} exactly one *zero* entry.

The *volume* of a lattice Λ , denoted $V(\Lambda)$, is inversely proportional to the number of lattice points per unit volume. More precisely, $V(\Lambda)$ may be defined as the volume of the *fundamental parallelogram* $\Pi(\Lambda)$ in \mathbb{R}^2 , which is given by

$$\Pi(\Lambda) \stackrel{\text{def}}{=} \{\xi_1 v_1 + \xi_2 v_2 : 0 \leq \xi_i < 1, i = 1, 2\}$$

There is a simple expression for the volume of Λ , namely, $V(\Lambda) = |\det \mathbf{G}|$.

We say that Λ induces a *lattice tiling* of S if the lattice points can be taken as the set \mathcal{T} to form a tiling (\mathcal{T}, S) .

D. Cyclic Arrays and Periods

We are now in a position to define the period of a doubly periodic array and to define cyclic two-dimensional arrays. Let \mathcal{A} be a doubly periodic two-dimensional array. Let (π_1, π_2) and (ξ_1, ξ_2) two linearly independent vectors such that each $i, j \in \mathbb{Z}$ satisfy $\mathcal{A}(i + \pi_1, j + \pi_2) = \mathcal{A}(i + \xi_1, j + \xi_2) = \mathcal{A}(i, j)$. Let s be the volume of the lattice formed from (π_1, π_2) and (ξ_1, ξ_2) . Let (π_3, π_4) and (ξ_3, ξ_4) be two linearly independent vectors for which, each $i, j \in \mathbb{Z}$ satisfy $\mathcal{A}(i + \pi_3, j + \pi_4) = \mathcal{A}(i + \xi_3, j + \xi_4) = \mathcal{A}(i, j)$. Let s' be the volume of the lattice formed from (π_3, π_4) and (ξ_3, ξ_4) . If $s' \geq s$ for each such pair of linearly independent vectors then we say that $\{(\pi_1, \pi_2), (\xi_1, \xi_2)\}$ is the *period* of \mathcal{A} and s is the *volume* of \mathcal{A} . The period in the one-dimensional case has the role of the period and the volume in the two-dimensional case.

Clearly, the period of a two-dimensional array is not unique. The volume of the array is unique and can be calculated from the given period. We have a theorem in the two-dimensional case which is akin to Theorem 2.

Theorem 3: Let \mathcal{A} be a doubly periodic array with period $\{(\pi_1, \pi_2), (\xi_1, \xi_2)\}$. Let (π_3, π_4) and (ξ_3, ξ_4) be two linearly independent vectors for which, each $i, j \in \mathbb{Z}$ satisfy $\mathcal{A}(i + \pi_3, j + \pi_4) = \mathcal{A}(i + \xi_3, j + \xi_4) = \mathcal{A}(i, j)$. Let s' be the volume of the lattice formed from (π_3, π_4) and (ξ_3, ξ_4) . If s is the volume of the lattice formed from (π_1, π_2) and (ξ_1, ξ_2) then s divides s' .

A shape S will be called *cyclic* if there is a lattice tiling Λ for S . In a cyclic sequence the order of the elements, in the sequence, is obvious. It is less obvious for a two-dimensional shape. We will discuss this order in Section IV.

III. TWO-DIMENSIONAL SYNCHRONIZATION ARRAYS

Several types of two-dimensional synchronization arrays are defined in the literature. We start we a general definition which was given in [3], [5]. Let S be a given shape, on the square grid, with m dots on grid points. S is called

a *distinct difference configuration* (DDC) if the $\binom{m}{2}$ lines connecting dots are distinct either in their length or in their slope. Several types of DDCs were defined in the literature. The main focus of research which was done on this topic is related to Costas arrays. A *Costas array* is an $m \times m$ permutation array having exactly one dot in each row and each column. Some results on Costas arrays are given in [12], [13], [19], [20], [21].

We now present a definition for a doubly periodic DDC. A *doubly periodic S-DDC* is a doubly periodic two-dimensional array \mathcal{A} with period $\{(\pi_1, \pi_2), (\xi_1, \xi_2)\}$ such that the following three properties are satisfied.

- The lattice formed by (π_1, π_2) and (ξ_1, ξ_2) is a lattice tiling for \mathcal{S} .
- Each copy of \mathcal{S} on the two-dimensional arrays \mathcal{A} is a DDC.
- In each two copies of \mathcal{S} in the tiling, the positions of the dots are the same.

Doubly periodic DDCs and in particular Costas array were considered in the past, e. g. [4], [22], [23]. There are two essential constructions for Costas arrays, both of them form doubly periodic DDCs. The first construction is due to Welch and the second Construction is due to Golomb (with a variant of Lempel) [12], [13], [19]. We will present both of them in their doubly periodic version.

The periodic Welch Construction:

Let α be a primitive root modulo a prime p and let \mathcal{A} be the square grid. For any integers i and j , there is a dot in $\mathcal{A}(i, j)$ if and only if $\alpha^i \equiv j \pmod{p}$.

Theorem 4: Let \mathcal{A} be the array of dots from the Periodic Welch Construction. Then \mathcal{A} is a doubly periodic \mathcal{S} -DDC with period $\{(0, p), (p-1, 0)\}$ and \mathcal{S} is a $p \times (p-1)$ rectangle.

The periodic Golomb Construction:

Let α and β be two primitive elements in $\text{GF}(q)$, where q is a prime power. For any integers i and j , there is a dot in $\mathcal{A}(i, j)$ if and only if $\alpha^i + \beta^j = 1$.

Theorem 5: Let \mathcal{A} be the array of dots from the Periodic Golomb Construction. Then \mathcal{A} is a doubly periodic \mathcal{S} -DDC with period $\{(0, q-1), (q-1, 0)\}$ and \mathcal{S} is a $(q-1) \times (q-1)$ square.

There are many important questions concerning Costas arrays. A few of them are related to the periodicity of the arrays. In particular we have the following two question:

- 1) Is the Welch construction generates all singly periodic Costas arrays? where a singly periodic Costas array of order n is an $n \times \infty$ array in which each $n \times n$ sub-array is a Costas array. Welch Construction has this property for $n = p - 1$.
- 2) Are there more constructions for Costas arrays with periodicity property?

The conjecture is NO for both questions. Some evidence that this conjecture is true is given in [24]. In fact it should be said that is very likely that most if not all Costas arrays are known since they derived from the known constructions [25]. In what follows we will throw more evidence for the difficulty to produce new doubly periodic \mathcal{S} -DDCs with many dots, different from those constructed by folding [4].

Costas arrays are only one family of DDCs, and doubly periodic DDCs. Two other families which were considered in the literature, are the sonar sequences [12], [15], [22], [26], and the Golomb rectangles [14], [17].

IV. THE FOLDING AND UNFOLDING METHODS

This section is devoted to with a transformation of a periodic sequence into a doubly periodic array and a transformation of a doubly periodic array into a periodic sequence. The two transformations will be called folding and unfolding, respectively, and as one might expect these two transformations are inverse of each other. As a consequence of the definition of folding we will be able to define the order of the elements in a cyclic shape. We will give the known theorems on the necessary and sufficient conditions that a folding exists. Based on these results we will define the inverse operation of unfolding. This will lead to the main theorem which will state when a doubly periodic two-dimensional DDC (or a cyclic DDC) is unfolded into a Sidon sequences.

The definition of folding involves a lattice tiling $(\mathcal{T}, \mathcal{S})$, where \mathcal{S} is the shape on which the folding is performed. A *direction* is a nonzero integer vector (d_1, d_2) , where $d_1, d_2 \in \mathbb{Z}$.

Let \mathcal{S} be a two-dimensional shape and let $\delta = (d_1, d_2)$ be a direction. Let Λ be a lattice tiling for a shape \mathcal{S} , and let \mathcal{S}_1 be the copy of \mathcal{S} , in the related tiling, which includes the origin. We define recursively a *folded-row* starting in the origin. If the point (i_1, i_2) is the current point of \mathcal{S}_1 in the folded-row, then the next point on its folded-row is defined as follows:

- If the point $(i_1 + d_1, i_2 + d_2)$ is in \mathcal{S}_1 then it is the next point on the folded-row.
- If the point $(i_1 + d_1, i_2 + d_2)$ is in $\mathcal{S}_2 \neq \mathcal{S}_1$ whose center is in the point (c_1, c_2) then $(i_1 + d_1 - c_1, i_2 + d_2 - c_2)$ is the next point on the folded-row (by Lemma 1 this point is on \mathcal{S}_1).

The definition of folding is based on a lattice Λ , a shape \mathcal{S} , and a direction δ . The triple $(\Lambda, \mathcal{S}, \delta)$ defines a folding if the definition yields a folded-row which includes all the elements of \mathcal{S} . It appears that only Λ and δ determines whether the triple $(\Lambda, \mathcal{S}, \delta)$ defines a folding. The role of \mathcal{S} is only in the order of the elements in the folded-row; and of course Λ must define a lattice tiling for \mathcal{S} .

The first two lemmas proved in [4] are an immediate consequence of the definitions and provide us concise conditions whether the triple $(\Lambda, \mathcal{S}, \delta)$ defines a folding.

Lemma 2: Let $(\mathcal{T}, \mathcal{S})$ be a lattice tiling defined by the two-dimensional lattice Λ and let $\delta = (d_1, d_2)$ be a direction. $(\Lambda, \mathcal{S}, \delta)$ defines a folding if and only if the set $\{(i \cdot d_1, i \cdot d_2) - c(i \cdot d_1, i \cdot d_2) : 0 \leq i < |\mathcal{S}|\}$ contains $|\mathcal{S}|$ distinct elements.

Lemma 3: Let $(\mathcal{T}, \mathcal{S})$ be a lattice tiling defined by the two-dimensional lattice Λ and let $\delta = (d_1, d_2)$ be a direction. $(\Lambda, \mathcal{S}, \delta)$ defines a folding if and only if $(|\mathcal{S}| \cdot d_1, |\mathcal{S}| \cdot d_2) - c(|\mathcal{S}| \cdot d_1, |\mathcal{S}| \cdot d_2) = (0, 0)$ and for each i , $0 < i < |\mathcal{S}|$ we have $(i \cdot d_1, i \cdot d_2) - c(i \cdot d_1, i \cdot d_2) \neq (0, 0)$.

The next theorem determine precisely when the triple $(\Lambda, \mathcal{S}, \delta)$ defines a folding.

Theorem 6: Let Λ be a lattice whose generator matrix is given by

$$\mathbf{G} = \begin{bmatrix} v_{11} & v_{12} \\ v_{21} & v_{22} \end{bmatrix},$$

where all the entries of \mathbf{G} are nonzeros. Let d_1 and d_2 be two positive integers and $\tau = \text{g.c.d.}(d_1, d_2)$. If Λ defines a lattice tiling for the shape \mathcal{S} then the triple $(\Lambda, \mathcal{S}, \delta)$ defines a folding

- with the direction $\delta = (+d_1, +d_2)$ if and only if $\text{g.c.d.}(\frac{d_1 v_{22} - d_2 v_{21}}{\tau}, \frac{d_2 v_{11} - d_1 v_{12}}{\tau}) = 1$ and $\text{g.c.d.}(\tau, |\mathcal{S}|) = 1$;
- with the direction $\delta = (+d_1, -d_2)$ if and only if $\text{g.c.d.}(\frac{d_1 v_{22} + d_2 v_{21}}{\tau}, \frac{d_2 v_{11} + d_1 v_{12}}{\tau}) = 1$ and $\text{g.c.d.}(\tau, |\mathcal{S}|) = 1$;
- with the direction $\delta = (+d_1, 0)$ if and only if $\text{g.c.d.}(v_{12}, v_{22}) = 1$ and $\text{g.c.d.}(d_1, |\mathcal{S}|) = 1$;
- with the direction $\delta = (0, +d_2)$ if and only if $\text{g.c.d.}(v_{11}, v_{21}) = 1$ and $\text{g.c.d.}(d_2, |\mathcal{S}|) = 1$.

A direction δ for which $(\Lambda, \mathcal{S}, \delta)$ defines a folding also defines the order of the elements in a cyclic shape \mathcal{S} . This order is exactly the order of the elements in the folded-row. It is easy to verify that only $|\mathcal{S}| - 1$ directions should be considered for the existence of a folding. The order of elements on \mathcal{S} is clearly not unique as it was proved in [4] that if one direction defines a folding then $\phi(|\mathcal{S}|)$ directions define a folding (and they come in pairs of reverse order), where ϕ is the Euler totient function.

The unfolding operation is defined directly from the folding operation. Let Λ be a lattice tiling for a two-dimensional shape \mathcal{S} and a let δ be a direction, for which $(\Lambda, \mathcal{S}, \delta)$ defines a folding. Then the folded-row is the *unfolded sequence* generated from the shape \mathcal{S} . In the folding, the folded-row indicates to which position of the array, each element of a given one-dimensional sequence will be assigned. In the unfolding, the folded-row is actually an unfolded-row and it indicates to which position of the sequence, each element of the array is assigned. These definitions are completely natural and there is no surprise. What is more interesting is the following theorem which connects two-dimensional doubly periodic \mathcal{S} -DDCs with Sidon sequences.

Theorem 7: Let \mathcal{A} be a two-dimensional doubly periodic \mathcal{S} -DDC with period $\{(\pi_1, \pi_2), (\xi_1, \xi_2)\}$. Let Λ be the lattice tiling of \mathcal{S} formed from (π_1, π_2) and (ξ_1, ξ_2) . If δ is a direction for which $(\Lambda, \mathcal{S}, \delta)$ defines a folding then the folded-row generated by the unfolding of \mathcal{S} is a Sidon Sequence.

Proof: We will give a sketch of the proof. A proof with all the details will appear in the full version of this work. We assign colors to the points of the square grid as follows. The points of the shape \mathcal{S} whose center is in the origin (say \mathcal{S}_0) are assigned colors by the order of the folded-row, where the origin is assigned with a *zero*. Each other copy of \mathcal{S} in the tiling is assigned with the same colors as \mathcal{S}_0 in the same related positions.

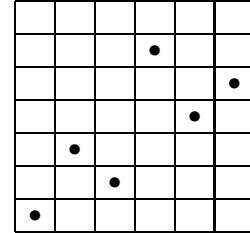
Assume the contrary, that the folded-row is not a Sidon sequence. It follows that there exists two distinct pairs of integers (i_1, i_2) and (i_3, i_4) , where i_1, i_2, i_3 , and i_4 , are positions with dots on the folded-row, such that $i_4 - i_3 \equiv i_2 - i_1 \pmod{n}$, where $n = |\mathcal{S}|$. Let \mathcal{S}_j , $1 \leq j \leq 4$, a copy of \mathcal{S} on the grid in which a point colored with i_j is the center. It can be shown that in one of these four copies the two pair of lines which connects the points colored with i_1 and i_2 ad those colored with i_3 and i_4 are equal in length and slope. A contradiction to the assumption that \mathcal{A} is a two-dimensional doubly periodic \mathcal{S} -DDC. ■

In [4] the following theorem was proved.

Theorem 8: Let Λ be a lattice tiling for a two-dimensional shape \mathcal{S} , $n = |\mathcal{S}|$, and let δ be a direction. Let \mathcal{B} be a Sidon sequence with m elements over \mathbb{Z}_n . If $(\Lambda, \mathcal{S}, \delta)$ defines a folding then there exists a two-dimensional doubly periodic \mathcal{S} -DDC \mathcal{A} with m dots in each copy of \mathcal{S} of \mathcal{A} .

In view of Theorems 7 and 8 it is tempting to prove that "a Sidon sequence over \mathbb{Z}_n with m elements exists if and only if a two-dimensional doubly periodic \mathcal{S} -DDC with m dots in each copy of \mathcal{S} exists". But, this claim is not correct. As we will conclude from the following discussion, which applies Theorem 7 on the known doubly periodic constructions for Costas Arrays.

Example 1: The following 7×6 array was obtained by the periodic Welch Construction for $p = 7$ and the primitive root 3 modulo 7.



By using unfolding with direction $(1, 1)$, where the lower left dot is taken on the origin we obtain the Sidon sequence $\{0, 8, 10, 11, 33, 37\}$ modulo 42.

Remark 1: A construction such as the periodic Golomb Construction cannot produce any Sidon sequence since the shape \mathcal{S} is a square and there is no direction which defines a folding when \mathcal{S} is a square.

V. NEW OPTIMAL SIDON SEQUENCES

The two celebrating constructions of optimal Sidon sequences are the ones of Singer [27] and Bose [28]. Let q be a power of a prime number. Singer's construction, which is based on projective planes, produces a Sidon sequence with $q + 1$ elements over \mathbb{Z}_{q^2+q+1} . Bose's construction, which is based on affine planes, produces a Sidon set with q elements over \mathbb{Z}_{q^2-1} . The construction of Ruzsa [29] generates optimal Sidon sequences with $p-1$ elements taken modulo $p^2 - p$, where p is a prime number. In this section we generalize this construction to obtain a Sidon sequence with $q - 1$ elements taken over $(q - 1) \times \text{GF}(q)$, where q is any power of a prime. Given a power of a prime q and a primitive element α in $\text{GF}(q)$, we construct the set $\mathcal{A}_{q,\alpha}$

defined by

$$A_{q,\alpha} = \{(i, \alpha^i) : 0 \leq i \leq q-2\}$$

Theorem 9: The set $A_{q,\alpha}$ is an optimal Sidon sequence.

Proof: We have to prove that given four integers i_1, i_2, i_3 , and i_4 , $0 \leq i_1, i_2, i_3, i_4 \leq q-2$, such that $i_1 \neq i_3$ and $i_2 \neq i_4$ then the two pairs $(i_1 + i_2, \alpha^{i_1} + \alpha^{i_2})$ and $(i_3 + i_4, \alpha^{i_3} + \alpha^{i_4})$ are not equal. Assume the contrary, that for four such integers we have

$$i_1 + i_2 \equiv i_3 + i_4 \pmod{q-1}, \quad \alpha^{i_1} + \alpha^{i_2} = \alpha^{i_3} + \alpha^{i_4}. \quad (2)$$

Let $t \equiv i_1 - i_3 \equiv i_4 - i_2 \pmod{q-1}$, where clearly we can assume that $0 < t < q-1$. Hence, we replace (2) with the equations

$$i_1 - i_3 \equiv i_4 - i_2 \pmod{q-1}, \quad \alpha^{i_1} - \alpha^{i_3} = \alpha^{i_4} - \alpha^{i_2} \quad (3)$$

We can substitute $i_1 \equiv i_3 + t \pmod{q-1}$ and $i_4 \equiv i_2 + t \pmod{q-1}$ in (3) to obtain the equation

$$\alpha^{t+i_3} - \alpha^{i_3} = \alpha^{t+i_2} - \alpha^{i_2},$$

which is equivalent to the equation

$$\alpha^{i_3}(\alpha^t - 1) = \alpha^{i_2}(\alpha^t - 1). \quad (4)$$

Since $0 < t < q-1$, it follows that $\alpha^t - 1 \neq 0$ and hence from (4) we have that $\alpha^{i_3} = \alpha^{i_2}$, i.e., $i_3 = i_2$ which contradicts the original choice of i_2 and i_3 . Therefore, $A_{q,\alpha}$ is a Sidon sequence. The optimality of the sequence is a straight forward enumeration. ■

Remark 2: The new construction of Sidon sequences does not help in constructing new doubly periodic \mathcal{S} -DDC since the abelian group is not \mathbb{Z}_n .

VI. CONCLUSIONS AND FUTURE RESEARCH

Sidon sets have many applications in coding theory and in communication problems. Constructions of optimal Sidon sequences are rare. We defined periodicity and cyclic arrays in the two-dimensional case. We proved that unfolded optimal doubly periodic two-dimensional synchronization patterns are optimal Sidon sequences. Thus, forming some equivalence between the two structures. All the results concerning two-dimensional arrays are generalized readily to higher dimensions. We presented a new construction of optimal Sidon sequences, with $q-1$ elements, over an alphabet with $q(q-1)$ elements, where q is a power of a prime. The main problem for future research in this direction is to find new constructions for optimal doubly periodic DDCs and new constructions for optimal Sidon sequences.

ACKNOWLEDGMENT

This work was supported in part by the United States-Israel Binational Science Foundation (BSF), Jerusalem, Israel, under Grant No. 2006097.

REFERENCES

- [1] A. E. Brouwer, J. B. Shearer, N. J. A. Sloane, and W. D. Smith, "A new table of constant weight codes", *IEEE Trans. Inform. Theory*, vol. 36, pp. 1334–1380, November 1990.
- [2] R. M. Roth and G. Seroussi, "Location-Correcting Codes", *IEEE Trans. Inform. Theory*, vol. 42, pp. 554–565, March 1996.
- [3] S. R. Blackburn, T. Etzion, K. M. Martin, and M. B. Paterson, "Two-Dimensional Patterns with Distinct Differences – Constructions, Bounds, and Maximal Anticodes", *IEEE Trans. on Inform. Theory*, vol. IT-56, pp. 1216–1229, March 2010.
- [4] T. Etzion, "Sequence folding, lattice tiling, and multidimensional coding", *IEEE Trans. on Inform. Theory*, to appear.
- [5] S. R. Blackburn, T. Etzion, K. M. Martin, and M. B. Paterson, "Distinct difference configurations: multihop paths and key predistribution in sensor networks", *IEEE Trans. on Inform. Theory*, vol. IT-56, pp. 3961–3972, August 2010.
- [6] A. Barg and A. Mazumdar, "Codes in permutations and error correction for rank modulation", *IEEE Trans. on Inform. Theory*, vol. IT-56, pp. 3158–3165, July 2010.
- [7] K. O'Bryant, "A complete annotated bibliography of work related to Sidon sequences", *The Elec. J. of Combin.*, DS11, pp. 1–39, July 2004.
- [8] W. C. Babcock, "Intermodulation interference in radio systems," *Bull. Sys. Tech. Journal*, pp. 63–73, June 1953.
- [9] G. S. Bloom and S. W. Golomb, "Applications of numbered undirected graphs", *Proceedings of the IEEE*, vol. 65, pp. 562–570, April 1977.
- [10] M. D. Atkinson, N. Santoro, and J. Urrutia, "Integer sets with distinct sums and differences and carrier frequency assignments for nonlinear repeaters", *IEEE Transactions on Communications*, vol. COM-34, pp. 614–617, 1986.
- [11] A. W. Lam and D. V. Sarwate, "On optimum time-hopping patterns", *IEEE Transactions on Communications*, vol. COM-36, pp. 380–382, 1988.
- [12] S. W. Golomb and H. Taylor, "Two-dimensional synchronization patterns for minimum ambiguity", *IEEE Trans. Inform. Theory*, vol. IT-28, pp. 600–604, 1982.
- [13] S. W. Golomb and H. Taylor, "Constructions and properties of Costas arrays", *Proceedings of the IEEE*, vol. 72, pp. 1143–1163, 1984.
- [14] J. P. Robinson, "Golomb rectangles", *IEEE Trans. Inform. Theory*, vol. IT-31, pp. 781–787, 1985.
- [15] R. A. Games, "An algebraic construction of sonar sequences using M-sequences", *SIAM Journal on Algebraic and Discrete Methods*, vol. 8, pp. 753–761, October 1987.
- [16] A. Blokhuis and H. J. Tiersma, "Bounds for the size of radar arrays", *IEEE Trans. Inform. Theory*, vol. IT-34, pp. 164–167, January 1988.
- [17] J. P. Robinson, "Golomb rectangles as folded ruler", *IEEE Trans. Inform. Theory*, vol. IT-43, pp. 290–293, 1997.
- [18] S. R. Blackburn, T. Etzion, K. M. Martin, and M. B. Paterson, "Efficient key predistribution for grid-based wireless sensor networks," *Lecture Notes in Computer Science*, vol. 5155, pp. 54–69, August 2008.
- [19] R. A. Games, "Algebraic constructions for Costas arrays", *Journal Combinatorial Theory, Ser. A*, vol. 37, pp. 13–21, 1984.
- [20] K. Drakakis, "A review of Costas arrays", *J. Appl. Math.*, vol. ???, pp. 1–32, 2006.
- [21] S. W. Golomb and G. Gong, "The status of Costas arrays", *IEEE Trans. Inform. Theory*, vol. 53, pp. 4260–4265, November 2007.
- [22] O. Moreno, S. W. Golomb, and C. Corrada, "Extended sonar sequences", *IEEE Trans. Inform. Theory*, vol. 43, pp. 1999–2005, November 1997.
- [23] O. Moreno and S. Golomb, "A new optimal double periodical construction of one target two-dimensional arrays", *40th Annual Conference on Information Sciences and Systems*, pp. 518–522, March 2006.
- [24] T. Etzion, S. W. Golomb, and H. Taylor, "Tuscan- k squares", *Advances in Applied Mathematics*, vol. 10, pp. 164–174, 1989.
- [25] K. Drakakis, F. Iorio, and S. Rickard "The enumeration of Costas arrays of order 28", *Information Theory Workshop*, Dublin, September 2010.
- [26] P. Erdős, R. Graham, I. Z. Ruzsa, and H. Taylor, "Bounds for arrays of dots with distinct slopes or lengths", *Combinatorica*, vol. 12, pp. 39–44, 1992.
- [27] J. Singer, "A theorem in finite projective geometry and some applications to number theory", *Trans. Amer. Math. Soc.*, vol. 43, pp. 377–385, 1938.
- [28] R. C. Bose, "An affine analogue of Singer's theorem", *J. Indian Math. Soc. (N.S.)*, vol. 6, pp. 1–15, 1942.
- [29] I. Z. Ruzsa "Solving a linear equation in a set of integers", *Acta Arith.*, vol. 65, pp. 259–282, 1993.